APPLICATION FOR PATENT

5

Secure User Action Request Indicator

10

Inventor: Mikko Lukkaroinen and Virve Inget

15

20

25

Background of the Invention

Communications devices, such as mobile phones, pagers and the like, are being packed with more and more features. In the past such mobile equipment has been a closed environment namely, all of the features use software within the mobile equipment or SIM. With the advent of new technologies, which use wireless communications protocols, such as Wireless Application Protocol (WAP) or comparable protocols, additional applications are accessible by the mobile device, from network servers. As a result a new security threat arises for mobile equipment. Mobile equipment will soon be subject to queries designed to extract confidential security information from the user, such as a PIN or other identifier. It is therefore necessary to devise a reliable system in which requests for information originating from remote "hostile" sources can be readily identified, ignored.

It is a purpose of this invention to provide a system for identifying remote inquiries which may precipitate a breach of security in the use of mobile equipment such as a mobile telephone, pager or other similar communications device.

Summary of the Invention

In order to use applications accessible from a network server, a mobile device is designed for

2

interactive use. This enables the mobile device to run such applications stored on a network server remote from the mobile device. To reduce the risk of receiving bogus requests for confidential identifiers, a system is designed to identify externally generated inquiries. To this end, means are provided to segregate the display of remote information requests. The mobile device is equipped with a display that is divided into dynamic and static display zones. Externally generated inquiries can be written only to the dynamic zone. Internally generated inquiries will trigger an indicator in the static zone to advise the user of the authenticity of the inquiry. As a result hostile requests for information may be immediately recognized and ignored.

Description of the Drawing

The invention is described in more detail below with reference to the attached drawing in which:

Figure 1 is a block diagram of a communication system utilizing the subject invention;

Figure 2 is a information flow diagram of the method of this invention; and

Figures 3a and 3b illustrate embodiments of the segregated screen of this invention.

Description of the Preferred Embodiment

5   The basic components of the communications system of
this invention are shown in the block diagram of figure 1.
A mobile device 1 is connected through a communications
link 9 to a network server 10.   In this instance, the
network server 10 does more than facilitate communications
10   traffic, it also provides interactive applications such as
banking, E-mail, investing and other features.

       Mobile device 1 includes a microprocessor control
unit (MCU) 2 that is accessed by the user via a user
15   interface 3, such as a keyboard.   Display 5 communicates
information from the MCU 2 to the user.   The MCU 2
contains the required software or firmware to execute the
functions on mobile device 2 required to operate the
applications resident in the network server 10.   Many of
20   the applications will require the use of security
identifiers, such as PINS and other confidential codes to
be access the personal application files of the user.

       In the early days of networked computers, there was a
25   proliferation of bogus log-in procedures that generated
inquiries to the personal computer for confidential
information.   If the information was supplied, it was
stolen and used for criminal or other activities not
authorized by the user.   The risk of such security
30   breaches is now becoming a problem for the user of mobile

devices, especially those equipped to take advantage of the communications protocols such as WAP. Such protocols represent standard operating procedures for interactive transmittal of data used to execute an assortment of

5   transactions. Although many of these transactions are secure because of the required digital signatures, such as PIN codes, it is essential that the code be maintained confidential. Bogus inquiries are a significant threat to the usefulness of these applications.

10

The mobile device 1 of this invention is equipped with a display 5, which is divided into two discrete zones, a static display zone 7 and a dynamic display zone 6. An internal display router 4 directs internally

15   generated inquiries and information to either the static or dynamic displays.

As shown in figures 3a and 3b, the static display 7 may present menu icons, tool symbols, status indications,

20   such as battery level, and other administrative references. The dynamic display 6 is for displaying interactive information relative to executing the activities of an application in progress. Information generated within the mobile device, may be displayed on

25   either the static or dynamic displays.

Information transmitted to the mobile device 1 from, for example a hostile source 11 through the network server 10, will utilize browser protocols and be readily

30   identifiable. This information is directed to the dynamic

5

display 6 by a external display router 8. In this manner, information from the network server 10 is isolated from the internally generated information of the mobile device 1.

5

To inform the user of the authenticity of inquiries for identifier codes, an indicator symbol 12, for example a blinking icon, will be displayed in the static display 7, as shown in figures 3a and 3b. When displayed, this
10 symbol will indicate to the user that the request is internally generated. Since the MCU identifies the external inquiry and this information is only routed to the dynamic display 6, there is a reliable indication that a PIN number can be transmitted without appreciable risk
15 of abuse.

As shown in figure 2, in operation, if a bogus log-in procedure from hostile source 11 is transmitted through the network server 10, when it is received, it is
20 identified by the MCU and routed only to dynamic display 6. The externally generated inquiry may be written only to the dynamic display 6. When an inquiry is generated by the execution of internal software, an indication is prominently displayed in the static display 7. When
25 responding to the inquiry displayed in dynamic display 6, the user will be warned not to respond unless the internal indicator is displayed.

In this manner transmittal of confidential
30 identification codes, restricted and the risk of

6

unauthorized interception and use of PIN codes and the like may be significantly reduced.